Published and Copyright (c) 1999 - 2013
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat
François Le Coat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1513 03/29/13

~ New York's Amazon Tax! ~ People Are Talking! ~ ARAnym Minipack!
~ Dismiss Ceglia Case? ~ Windows Blue Preview! ~ Year of the Hack!

~ Sweden Axes "New Word" ~ Spamhaus DDOS Attack! ~ Ouya Ships in June!
~ New Steve Jobs Book! ~ ~ Windows Blue Leaks!

-* EA Reveals SimCity Apology! *-
-* US Restricts Purchases of Chinese IT *-
-* Mozilla Is Unlocking The Power of the Web! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

Hey, we've managed to make it through an entire week without any snow! Could we really be seeing the true beginning of the Spring season? I certainly hope so! So, while we can, let's enjoy it!

Until next week...

=~=~=~=

ARAnyM MiniPack

Hi,

ARAnyM <http://aranym.org/> is the GNU/GPL ATARI Virtual Machine from which a minimal configuration, the *miniPack* is distributed <http://eureka.atari.org/miniPack.zip> miniPack is modified with the new releases of freeMiNT 1.18.0. It supports :

'Run_win' allows launching on PC with Windows
'MacAranym' allows launching on PPC Macintosh with OS X
'MacAranym JIT' allows launching on IntelMac with OS X
'run_x86.sh' allows launching on PC with x86-Linux
'run_ppc.sh' allows launching on Mac _and_ PS3 with PPC-Linux

So Macintosh-PC-PlayStation3 are all supported with Windows, OS X and GNU/Linux.

This simple ARAnyM configuration is running on any machine.
Here is a screen-shot <http://eureka.atari.org/aranym.gif>

Enjoy, it's yours =)

--
François LE COAT
Author of Eureka 2.12 (2D Graph Describer, 3D Modeller)
<http://eureka.atari.org/>

=~=~=~=

->In This Week’s Gaming Section - EA Reveals Free SimCity Apology Games!
Ouya Game Console Ships in June!
Mozilla Unlocking The Power!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!

EA Reveals Free SimCity Apology Games

EA has revealed the list of eight Origin games that will be offered to owners of SimCity for free, by way of an apology for the game’s teething issues.

Last week, the company apologised for the continuing connection and server issues players were experiencing and stated that everyone who registers the game before March 25 will be allowed to choose one Origin game from a list of eligible titles to download for free.

We re humbled by your patience and passion for the game. Thanks for building something very special with us, together.

The eligible titles are Battlefield 3 (Standard Edition), Bejeweled 3, Dead Space 3 (Standard Edition), Mass Effect 3 (Standard Edition), Medal of Honor Warfighter (Standard Edition), Need For Speed Most Wanted (Standard Edition), Plants vs. Zombies and SimCity 4 Deluxe Edition. You’ll have until March 30 to claim your free game.

The post also includes an explanation from developers Maxis, which reads, "At Maxis, our studio values dictate that we innovate and create something that is quirky, complex and challenging. Sometimes this bites us in the butt, but our servers are green and we re seeing record numbers of players all online and having a great time.

"We re getting great feedback from our fans and know that many of you are having fun and exploring this whole new expression of SimCity. We re humbled by your patience and passion for the game. Thanks for building something very special with us, together."

It’s true that most of the game’s issues seem to be resolved; the company recently restored the non-essential features it disabled to ease the strain on the servers. Despite this, there are still no plans to introduce the offline mode many fans have asked for.

Is this gesture enough to compensate you for the troubles you experienced, or have you given up on SimCity? Let us know what you think and which

game you'll be getting in the comments below.

Ouya Game Console Ships To Kickstarter Backers; Sales Begin June 4

Ouya, the world's first game console to be funded on the Kickstarter crowd-funding website, began shipping to people who donated at least $95 through Kickstarter today.

If you didn't back Ouya on Kickstarter, you won't be able to get one just yet. Sales to the general public start on June 4, and both Ouya and its retail partners - including Amazon, Target, and Best Buy - are taking preorders right now. The console costs $99, and additional wireless controllers are priced at $49 each.

How does Ouya compare to the PlayStation and Xbox?

Ouya's much cheaper and smaller (it's about the size of a Rubik's cube), and has fewer games right now. It's also less powerful; while it can play 1080p games on an HD television, the graphics quality isn't quite as good as the most demanding current-gen games.

What are Ouya's tech specs like?

It uses the Tegra 3 chipset, which is the same one used in Google's "designed with gaming in mind" Nexus 7 tablet. It also has 8 GB of internal storage, which is about as much as the cheaper Xbox 360 or Wii U models have. This is enough for a couple of dozen smaller games, or a small handful of larger ones. Additional storage can be added via USB.

What kind of games are available for Ouya?

A total of 104 games are available so far, many of them written just for Ouya but some familiar to Android tablet owners. Perhaps the most recognizable game is Square-Enix's Final Fantasy III, which appeared on the Nintendo DS and Sony PlayStation Portable before it showed up on Android (and also costs more than most Android games).

Ouya's website says "Eight thousand [game] developers have created developer accounts," and that more games will be coming out in the near future.

Can you make your own games for Ouya?

Every Ouya has a "Make" button on its main menu, which lets you install games that you've either written yourself or downloaded from the Internet. You can use the free Ouya Development Kit to write Ouya games, the same way that you'd write Android games or apps.

What does it mean that they say the Ouya is "open?"

Ouya's website says that "we welcome you to unscrew it and have a look around," and Ouya has partnered with MakerBot to let you build your own custom case for it - if you can afford the $2,199 MakerBot 3D printer. MakerBot's website does not say whether third parties are allowed to sell custom cases they've printed.

Mozilla Is Unlocking The Power of the Web as a Platform for Gaming

Mozilla, a non-profit organization dedicated to promoting openness, innovation and opportunity on the Web, is advancing the Web as the platform for high-end game development. With Mozilla s latest innovations in JavaScript, game developers and publishers can now take advantage of fast performance that rivals native while leveraging scale of the Web, without the additional costs associated with third-party plugins. This allows them to distribute visually stunning and performance intensive games to billions of people more easily and cost effectively than before.

To make these advancements, Mozilla developed a highly-optimized version of JavaScript that supercharges a developer s gaming code in the browser to enable visually compelling, fast, 3D gaming experiences on the Web. With this technology we are also opening up the path for 3D Web-based games on mobile as JavaScript performance continues to close the gap with native.

Today, we are excited to unlock this technology for high-performance games, by teaming up with Epic Games. By leveraging this new JavaScript optimization technology, Mozilla has been able to bring Epic s Unreal Engine 3 to the Web. With this port, developers will soon be able to explore limitless possibilities when it comes to porting their popular gaming titles to the Web.

Mozilla was able to recently prove the Web is capable of being a compelling gaming platform with its BananaBread game demo, which is built using Web technologies Mozilla pioneered, including WebGL, Emscripten and now asm.js. The demo shows how high-end games can easily be ported to JavaScript and WebGL while still maintaining a highly responsive, visually compelling 3D gaming experience.

Developers wishing to test this technology can check out the latest version of BananaBread with its peer-to-peer, multiplayer WebRTC technology and JavaScript performance improvements. BananaBread works in all browsers that support WebGL.

As high-performance games on the Web move to rival native performance, Mozilla is also opening up the path to Web-based games on mobile. We are working with premium game publishers such as Disney, EA and ZeptoLab who are using the same technology to bring performance optimizations to their top-rated games.

Developers can submit fun games and apps to the Firefox Marketplace now. The Firefox Marketplace is currently available as a preview on Firefox for Android and will come to Firefox OS later this year.

=~=~=~=

U.S. Law To Restrict Government Purchases of Chinese IT Equipment

Congress quietly tucked in a new cyber-espionage review process for U.S. government technology purchases into the funding law signed this week by President Barack Obama, reflecting growing U.S. concern over Chinese cyber attacks.

The law prevents NASA, and the Justice and Commerce Departments from buying information technology systems unless federal law enforcement officials give their OK.

A provision in the 240-page spending law requires the agencies to make a formal assessment of "cyber-espionage or sabotage" risk in consultation with law enforcement authorities when considering buying information technology systems.

The assessment must include "any risk associated with such system being produced, manufactured or assembled by one or more entities that are owned, directed or subsidized" by China.

The U.S. imports a total of about $129 billion worth of "advanced technology products" from China, according to a May, 2012 report by the Congressional Research Service.

The amendment to the so-called "continuing resolution" to fund the government through September 30 originated in the Commerce, Justice and Science subcommittee of the House of Representatives, chaired by Virginia Republican Representative Frank Wolf.

It had gotten little attention until a blog post this week by Stewart A. Baker, a partner in the Washington office of Steptoe & Johhson and a former Assistant Secretary in the U.S. Department of Homeland Security.

Writing in the Volokh Conspiracy, one of the country’s most prominent legal blogs, Baker wrote on Monday that the measure "could turn out to be a harsh blow" for Chinese computer-maker Lenovo and also "bring some surprises for American companies selling commercial IT gear to the government."

U.S. concern about Chinese cyber-attacks has mounted in recent months, with top officials - including President Barack Obama - vocally condemning the practice.

Obama raised the issue in a phone call with Chinese President Xi Jinping earlier this month, and told ABC news in an interview that some cyber security threats are "absolutely" sponsored by governments.

"We’ve made it very clear to China and some other of the state actors that, you know, we expect them to follow international norms and abide by international rules," he said.

Xi said the United States and China should avoid making "groundless accusations" against each other about cyber-security and work together on the problem.

The exchange came after U.S. computer security company Mandiant said a secret Chinese military unit based in Shanghai was the most likely driving force behind a series of hacking attacks on the United States.

Last year, the House Intelligence Committee released a report urging U.S. telecommunication companies not to do business with Huawei Technologies Co Ltd and ZTE Corp because it said potential Chinese state influence on the companies posed a threat to U.S. security.

Both companies took issue with the report, which Huawei spokesman William Plummer called "baseless."

Plummer said in an email their reading of the bill is that it "does not apply to Huawei based on the description of covered entities."

Baker, a technology security lawyer, said he believed the language would live on in future appropriations bills and possibly get tougher over time.

"Once a provision ends up in the appropriations bill ... it tends to stay there unless there's a good reason to take it out," Baker said. "We could easily see (the appropriation committees) tighten up some of the language in the future."

China could challenge the measure as a violation of World Trade Organization rules, but may have a tough time making that case because it is not a member of the WTO agreement setting international rules for government procurement.

A Chinese government spokesman was not immediately available for comment.

The agreement also contains a national security exemption that would be another U.S. line of defense against a possible Chinese challenge, Baker said.

It is possible other countries could raise objections because of the potential for the provision to prevent purchases of Lenovo computers manufactured in Germany or Huawei handsets designed in Britain, he said.

But they may decide to tolerate it because of their own concerns about Chinese hacking, Baker said.

"The goal is not to hurt American and European companies that have operations in China," said a congressional aide who worked on the House bill where the wording originated. "It was really targeting entities that are directed by Beijing," said the aide, who asked not to be identified.

The federal government's purchases, which are funded by taxpayers' money, are often urged to give preference to vendors that offer the cheapest services.

The congressional aide said China may heavily subsidize some companies to present the U.S. market with a much lower price.

"It's a helpful reminder to look at the supply chain" of U.S. firms, the aide said. "The cheap option may be artificially lowered because potentially there are ulterior motives."

Judge Recommends Ceglia Case vs Facebook Be Dismissed

A federal judge on Tuesday recommended the dismissal of a lawsuit against

Facebook Inc in which Paul Ceglia, an upstate New York wood pellet salesman, claimed a huge ownership stake in the social media company.

U.S. Magistrate Judge Leslie Foschio said there is "clear and convincing evidence" that an alleged 2003 contract with Mark Zuckerberg, now Facebook's chief executive, that Ceglia claimed entitled him to a one-half interest in the company is a "recently created fabrication."

In October, federal prosecutors in Manhattan announced criminal mail and wire fraud charges against Ceglia, whom U.S. Attorney Preet Bharara accused of seeking "a quick pay day based on a blatant forgery.

Ceglia, who has lived in Wellsville, New York, pleaded not guilty. Each criminal charge carries a maximum sentence of 20 years in prison.

Paul Argentieri, a lawyer for Ceglia, was not immediately available on Tuesday for comment.

In his 2010 civil lawsuit, Ceglia claimed that a 2003 contract he signed with Zuckerberg, then a Harvard University freshman, entitled him to the Facebook stake.

Though Zuckerberg had done programming work for Ceglia's company StreetFax.com, Facebook maintained that a separate agreement involving that entity, which did not entitle Ceglia to a big Facebook stake, was the real contract between the two.

In a 155-page recommendation, Foschio said Ceglia's arguments largely consisted of "self-defeating inconsistencies" that established the "fraudulent nature" of his claims.

"Plaintiff has utterly failed to rebut the plethora of evidence establishing that it is highly probable and reasonable the StreetFax document was the operative contract," the Buffalo, New York-based judge wrote.

Foschio also said it is "highly probable and reasonably certain" that the contract Ceglia said was real was "fabricated for the express purpose of filing the instant action."

The case now goes to U.S. District Judge Richard Arcara, who will decide whether to approve Foschio's recommendation.

Colin Stretch, deputy general counsel of Facebook, said in a statement that Foschio's recommendation "confirms what we have said from day one: this lawsuit is an inexcusable fraud based on forged documents."

Facebook's market value is now about $60 billion.

The accusations against Facebook and Zuckerberg had been an unusual distraction during the Menlo Park, California-based company's march toward its May 2012 initial public offering.

Facebook's origin was also the focus of separate litigation by Zuckerberg's twin Harvard classmates Cameron and Tyler Winklevoss, chronicled in the 2010 movie "The Social Network."

Ceglia claimed that Zuckerberg shared his plans for a social networking website while working at StreetFax, and contracted to give him a stake in exchange for a $1,000 investment.

To build his case, Ceglia submitted what he said were emails from Zuckerberg that proved the pair discussed the project that eventually became Facebook.

But Facebook said Zuckerberg did not even conceive of the idea for a social media company until December 2003.

Its lawyers said Ceglia had produced fraudulent documents, citing work by forensic experts who concluded that he had typed text into a Microsoft Word document, and declared it the text of emails with Zuckerberg in 2004.

Ceglia went through a string of lawyers from prominent firms, including DLA Piper and Milberg, who worked with him on various parts of the civil case but later withdrew.

Earlier this month, Ceglia filed a separate civil lawsuit against Bharara and U.S. Attorney General Eric Holder to halt the criminal case.

The civil case is Ceglia v. Zuckerberg et al, U.S. District Court, Western District of New York, No. 10-00569. The lawsuit against Bharara and Holder is Ceglia v. Holder et al in the same court, No. 13-00256. The criminal case is U.S. v. Ceglia, U.S. District Court, Southern District of New York, No 12-cr-00876.

How To Survive The Year of The Hack

After three months of headlines from China to the White House and every geek haven in between, this week introduced the world to the cyber attack that may or may not be slowing down the entire Internet, followed by the digital assault on American Express. Yes, 2013 is already the year there were too many hacking incidents to keep track of, but "hacking" has also become a kind of catch-all for nefarious things done on a computer, and it’s becoming increasingly difficult to tell apart global headline from personal headache. That kind of vagueness has left average Internet users wondering whether they could be exposed to the same threats as major companies and government systems and has demonized "hackers" like Aaron Swartz, Matthew Keys, and Weev, who face(d) felonies and jail time for low level computer crimes. With more than a few different kinds of "hacks" dominating the news in just the last couple of weeks alone, it’s about time somebody defined the hacking headlines once and for all.

Fear Factor: Low-Medium. Once someone does get inside an email account, it can be scary just how quickly everything else falls apart. But the technique isn’t exactly computer science, and these types of hacks can be avoided if you have a safe enough email provider. Indeed, email lurkers have publicly exposed security flaws inside some of the most popular inboxes in the world; Guccifer, for the most part, has gone after AOL, Yahoo, and Comcast accounts, which don’t have very good security it only take a few personal details to get an AOL user to fork over a password. Careful password habits like using two-step verification should help the average non-Bush user fend off these kinds of security breaches.

Fear Factor: Medium. A lot of different levels of hackers use the link-doom method, from those creeps trying to take over unsuspecting women’s webcams to the secret unit apparently linked to the People’s Liberation Army in

China, which reportedly used very well concealed spear-phishing to get high level people inside various media outlets to download malware and use it for the purposes of international espionage at that drab looking building over there. For the average Twitter user, though, there are various ways to avoid downloading malware, even spear-phishing, which does a very good job at looking legitimate. But basically, don't click things that look fishy (or phishy), don't visit suspect forums, and don't buy suspect things. And make sure your computer's anti-malware program, scripts, and browsers are up to date.

What It Looks Like: This is another, more clandestine way to get people to download malware, and that was likely the type of hack (probably from China) that infiltrated the internal servers at Facebook, Apple, and possibly Twitter, as the companies reported, like dominoes, in February. This type of hack doesn't target an individual but a website that many individuals visit you know, like when the people visit the watering hole. When trying to target Facebook's developers, for example, hackers planted "malicious code injected into the HTML of the site used an exploit in Oracle's Java plug-in," as AllThingsD's Mike Isaac explained.

Fear Factor: High. Once you visit an infected site, well, that's pretty much the end of the attack. That's the thing that trips up a lot of people writing about and spreading fears around hacking, and the Facebooks and Twitters of the world are pretty good at protecting their accounts when they get played. But if you're looking for a solution, a lot of people have suggested that getting rid of Java might help your situation, since a lot of malware exploits that code deployment platform. Then again, it might not really be that easy, since the malware spreads so fast and to such large sites.

What It Looks Like: Denial-of-service attacks have received a lot of attention this week because of the fight between Spamhaus and Cyberbunker, which resulted in the biggest ever DDoS attack ever. These rapid-fire attacks, which infect computers with malware to overwhelm and then shut down websites, were also responsible for the big bank attacks over the last few months, including Thursday's AmEx breach, which likely came from an Iranian hacker group called the Izz ad-Din al-Qassam Cyber Fighters. That South Korean hack the other day from North Korea was also likely of the DDoS variety. And denials of service are getting more powerful. The AmEx hack, for example, infected "infected powerful, commercial data centers with sophisticated malware and directed them to simultaneously fire at each bank, giving them the horsepower to inflict a huge attack," as The New York Times's Nicole Perlroth and David Sanger explain.

Fear Factor: Very High. While some have accused the Times of being sensationalist with its use of "cyber warfare," the DDoS attacks have become more and more powerful, which is cause for concern. There are ways to close certain holes on the web's DNS servers that could ease the flood of relatively tame denial-of-service attacks, but when it comes to national security the U.S. is no match for China's hackers, who are trying to take down some of America's most crucial infrastructure. President Obama acknowledged the threat in his State of the Union address and recently met with major business leaders about cyber attacks. In addition to clandestine efforts to fight back against China's cyber fighters, though, the White House is now looking at something like sanctions: The latest government funding bill would make it harder for Chinese companies to sell tech products to a few federal agencies, according to Politico, although that's only minorly comforting. But Obama has ordered cyber attacks on Iran, after the famous Stuxnet worm targeted U.S. computer infrastructure.

What It Looks Like: Nothing like a vague legal term to get the people talking. "Unauthorized access" can blanket pretty much any computer related crime, as federal investigators have made blatantly clear in the high-profile cases of three men facing lots of prison time for not a lot of hacking. In theory, "unauthorized access" means getting into a person or an organization's computer even though you're not supposed to even though that's pretty much the point of hacking. But the term has been used very differently in accusing each of the three men: Swartz literally went inside an MIT server room and assigned himself IP addresses, Keys gave up some access to the content management system of the Los Angeles Times website, and it's not even clear what Weev accessed without authority. Many, many people, from inside the hacking community and out, have accused the government of using the "unauthorized access" charge to prove a point.

Fear Factor: Low. The scary part is how vague the definition of a not scary hacking act has become. Authorities and bigger organizations and businesses tend to fear these kinds of attacks more than individuals, because it's usually the individuals (or Anonymous) use the highly illegal tactics to make often mundane points of their own.

What It Looks Like: Forget cyber hacks, people are still hacking actual Internet cable lines! In an attempt to take an entire continent offline, three scuba diving hackers have now gone straight to the source and literally cut the chords in Egypt.

Fear Factor: Medium. It's definitely the most effective way to take out an entire country or continent's Internet. But, it's pretty conspicuous and not very precise. You've got to be a pretty smart underwater hacker to be an effective one.

There are certainly other types of "hacks" out there, but this should help clarify things the next time you're facing three frightening headlines about technology in one newspaper. China isn't coming after your Netflix account. But you should still probably dump that stupid password, beef up your email and computer security, and avoid the MIT server room. And the North Koreans. Those guys are up to no good.

New York High Court Upholds State's "Amazon Tax"

Amazon.com Inc and other out-of-state online retailers must collect state tax on New York state customers, the state's highest court ruled on Thursday, a decision at odds with other courts that could set the stage for a showdown in the U.S. Supreme Court.

The case, combining two brought by Amazon and Overstock.com Inc, was decided by the New York State Court of Appeals by a vote of 4-1.

"It's unfortunate and the (U.S.) Supreme Court ought to look at this," Overstock acting Chief Executive Jonathan Johnson told Reuters by phone.

"We have states saying different things," he said, citing a ruling by the Illinois Supreme Court that a similar tax was not permissible.

The U.S. Supreme Court typically accepts cases where lower courts issue conflicting opinions.

"The ruling by the New York Court of Appeals conflicts with both the U.S. Supreme Court's precedents and with contrary decisions by other state courts that have looked at the same issue," an Amazon spokesman said by email.

The best solution to that conflict, he said, would be passage of federal legislation currently under consideration that would allow any state to require tax collection.

New York State Commissioner of Taxation and Finance Thomas Mattox commended the court for "recognizing the logical application of existing precedent to the 21st Century economy."

Eight other states have passed legislation similar to New York's, which requires out-of-state retailers to collect sales tax even when they do not have a physical presence in the state, but do have affiliates in the state.

Retailers with a physical presence in any state must always remit sales tax on purchases made either in a store or online, but since a 1992 Supreme Court decision, Quill Corp v. North Dakota, retailers lacking a "nexus" of operation in a state have not been required to collect sales tax.

In recent years, as online sales have grown as a portion of the retail market, Amazon has agreed to begin collecting sales taxes in California, Texas, New Jersey and some other states where it has distribution facilities or plans to build them.

Richard Pomp, professor of law at the University of Connecticut and an expert on state taxes, said the decision was not a surprise, and will have less impact today than it would have before Amazon began cutting deals with states to pay taxes.

Overstock ended its affiliate network in New York in 2008 and so the ruling will not have an impact on its operations, Johnson said.

Amazon was already paying tax to the state pending the decision, according to the New York Department of Taxation.

Between the New York law's passage in 2008 and today, online-only retailers collected and remitted $500 million in sales tax on more than $6 billion in transactions, according to the New York State Department of Taxation and Finance.

The cases are Overstock.com v. New York State Department of Taxation and Finance, New York State Court of Appeals No. APL-2012-00017, and Amazon.com v. New York State Department of Taxation and Finance, New York State Court of Appeals No. APL-2012-00045.

Microsoft To Debut Windows Blue Preview This Summer

Microsoft is expected to announce the next generation of the Windows operating system later this year. According to The Verge, the company began working on a milestone preview version of Windows Blue earlier this month, and plan to make it available to developers and enthusiasts

at its Build developer conference in June. Microsoft earlier this week acknowledged the Blue codename, however it is unlikely that the final product will be called Windows Blue. Earlier rumors have suggested that the next version of Windows will include a variety of new features such as customized live tiles and improvements to the company s Snap View feature. Microsoft s Build developers conference is scheduled to take place on June 26th in San Francisco.

Windows Blue Leaks Online

An early build of Windows Blue, the next version of Windows, has leaked online on the same day that Microsoft CEO Steve Ballmer celebrates his 57th birthday. Build 9364, a partner version that was originally compiled on March 15th, has been made available on file sharing sites and includes some of the new changes that Microsoft is building into its significant Windows 8 update. Leaked screenshots posted at Winforum show that the company is bringing smaller tile arrangements and even a larger desktop one to its Start Screen, along with greater control over the color personalization options, and a whole lot more.

Microsoft is building in additional Snap Views into Windows Blue, allowing users to place apps side-by-side in the Windows 8 view. The new 50 / 50 view is similar to the desktop mode snapping, but Microsoft also supports up to 4 snapped apps alongside each other. New alarm, sound recorder, movie moments, and calculator WIndows 8 -style apps will also take advantage of these new views, but we understand developers will be able to update their apps to support the additional Snap Views alongside other API changes and additions. The snapping improvements also apply to multi monitor support, where you can now run individual Windows 8-style apps across multiple monitors.

Other improvements include a number of new options in the Windows 8-style settings screen. Microsoft appears to be adding all of the necessary settings required to ensure tablet users don’t have to drop to the desktop Control Panel to change things. SkyDrive options are present, which appear to show greater integration with auto camera uploads and control over device back ups and files. There’s also an app settings section that surfaces options to change default apps and information on app sizes.

Settings and UI improvements aside, Microsoft is also making changes to its Charms. The Devices Charm includes a new "play" option, which looks similar to the existing PlayTo options found in Windows 8. On the Share Charm there’s a new screenshot option that lets you quickly share an image with applications. Internet Explorer 11 is also included in Blue, although it’s not immediately clear from the leaked screenshots what improvements have been made. A tab sync feature appears in some screenshots, suggesting that Microsoft is planning to make tabs available on additional Windows Blue devices.

Touch users can also use new gestures throughout Windows Blue. On the Start Screen you can swipe up from the bottom to bring up a list of all apps, and in the desktop mode you can swipe up or down to reveal a desktop app bar that provides access to snap, projector settings, and more. We’re looking into other leaked features and screenshots so we’ll update you on any other additions. Windows Blue is expected to enter public preview over the coming months, with a full release due later this year.

Sweden Axes New Word after Google Intervenes

US search engine giant Google has successfully put pressure on the Swedish Language Council to remove an entry from its recently released list of new Swedish words.

In December, the council unveiled its customary annual list of new Swedish words. Among the words that Swedes had begun using in 2012 was "ogooglebar" (’ungoogleable’).

The California-based multinational soon got into a huff, asking the council to amend its definition. But the language experts refused to bow down to the demands, instead choosing a third option - removing the term altogether.

"Instead, we’re removing the word today and stating our displeasure with Google’s attempt to control the language," Language Council head Ann Cederberg said in a statement.

The word was to be used to describe something "that you can’t find on the web with the use of a search engine", according to the Language Council.

However, Google was less than thrilled that a word based on its name had been highlighted by Sweden’s "official language cultivation body".

Google wanted the council to specify that the word’s definition only covered searches performed using Google, and not searches involving other search engines.

The move marks the first time the Language Council has removed a word from its annual list, but the Swedish wordsmiths don’t think the word’s removal means it should be removed from the language itself.

"If we want to have ogooglebar in the language, then we’ll use the word and it’s our use that gives it meaning - not a multinational company exerting pressure. Speech must be free!" Cederberg said.

According to Cederberg, the Language Council could have compromised with Google’s requests, but decided to instead spark a debate.

"It would go against our principles, and the principles of language. Google has forgotten one thing: language development doesn’t care about brand protection."

The DDoS That Almost Broke the Internet

The New York Times morning published a story about the Spamhaus DDoS attack and how CloudFlare helped mitigate it and keep the site online. The Times calls the attack the largest known DDoS attack ever on the Internet. We wrote about the attack last week. At the time, it was a large attack, sending 85Gbps of traffic. Since then, the attack got much worse. Here are some of the technical details of what we’ve seen.

On Monday, March 18, 2013 Spamhaus contacted CloudFlare regarding an

attack they were seeing against their website spamhaus.org. They signed up for CloudFlare and we quickly mitigated the attack. The attack, initially, was approximately 10Gbps generated largely from open DNS recursors. On March 19, the attack increased in size, peaking at approximately 90Gbps. The attack fluctuated between 90Gbps and 30Gbps until 01:15 UTC on on March 21.

The attackers were quiet for a day. Then, on March 22 at 18:00 UTC, the attack resumed, peaking at 120Gbps of traffic hitting our network. As we discussed in the previous blog post, CloudFlare uses Anycast technology which spreads the load of a distributed attack across all our data centers. This allowed us to mitigate the attack without it affecting Spamhaus or any of our other customers. The attackers ceased their attack against the Spamhaus website four hours after it started.

Other than the scale, which was already among the largest DDoS attacks we've seen, there was nothing particularly unusual about the attack to this point. Then the attackers changed their tactics. Rather than attacking our customers directly, they started going after the network providers CloudFlare uses for bandwidth. More on that in a second, first a bit about how the Internet works.

The "inter" in Internet refers to the fact that it is a collection of independent networks connected together. CloudFlare runs a network, Google runs a network, and bandwidth providers like Level3, AT&T, and Cogent run networks. These networks then interconnect through what are known as peering relationships.

When you surf the web, your browser sends and receives packets of information. These packets are sent from one network to another. You can see this by running a traceroute. Here's one from Stanford University's network to the New York Times' website (nytimes.com):

```
1  rtr-servcore1-serv01-webserv.slac.stanford.edu (134.79.197.130)  0.572 ms
 2  rtr-core1-p2p-servcore1.slac.stanford.edu (134.79.252.166)  0.796 ms
 3  rtr-border1-p2p-core1.slac.stanford.edu (134.79.252.133)  0.536 ms
 4  slac-mr2-p2p-rtr-border1.slac.stanford.edu (192.68.191.245)  25.636 ms
 5  sunncr5-ip-a-slacmr2.es.net (134.55.36.21)  3.306 ms
 6  eqxsjrt1-te-sunncr5.es.net (134.55.38.146)  1.384 ms
 7  xe-0-3-0.cr1.sjc2.us.above.net (64.125.24.1)  2.722 ms
 8  xe-0-1-0.mpr1.sea1.us.above.net (64.125.31.17)  20.812 ms
 9  209.249.122.125 (209.249.122.125)  21.385 ms
```

There are three networks in the above traceroute: stanford.edu, es.net, and above.net. The request starts at Stanford. Between lines 4 and 5 it passes from Stanford's network to their peer es.net. Then, between lines 6 and 7, it passes from es.net to above.net, which appears to provide hosting for the New York Times. This means Stanford has a peering relationship with ES.net. ES.net has a peering relationship with Above.net. And Above.net provides connectivity for the New York Times.

CloudFlare connects to a large number of networks. You can get a sense of some, although not all, of the networks we peer with through a tool like Hurricane Electric's BGP looking glass. CloudFlare connects to peers in two ways. First, we connect directly to certain large carriers and other networks to which we send a large amount of traffic. In this case, we connect our router directly to the router at the border of the other network, usually with a piece of fiber optic cable. Second, we connect to what are known as Internet Exchanges, IXs for short, where a number of networks meet in a central point.

Most major cities have an IX. The model for IXs are different in different parts of the world. Europe runs some of the most robust IXs, and CloudFlare connects to several of them including LINX (the London Internet Exchange), AMS-IX (the Amsterdam Internet Exchange), and DE-CIX (the Frankfurt Internet Exchange), among others. The major networks that make up the Internet - Google, Facebook Yahoo, etc. - connect to these same exchanges to pass traffic between each other efficiently. When the Spamhaus attacker realized he couldn't go after CloudFlare directly, he began targeting our upstream peers and exchanges.

Once the attackers realized they couldn't knock CloudFlare itself offline even with more than 100Gbps of DDoS traffic, they went after our direct peers. In this case, they attacked the providers from whom CloudFlare buys bandwidth. We, primarily, contract with what are known as Tier 2 providers for CloudFlare's paid bandwidth. These companies peer with other providers and also buy bandwidth from so-called Tier 1 providers.

There are approximately a dozen Tier 1 providers on the Internet. The nature of these providers is that they don't buy bandwidth from anyone. Instead, they engage in what is known as settlement-free peering with the other Tier 1 providers. Tier 2 providers interconnect with each other and then buy bandwidth from the Tier 1 providers in order to ensure they can connect to every other point on the Internet. At the core of the Internet, if all else fails, it is these Tier 1 providers that ensure that every network is connected to every other network. If one of them fails, it's a big deal.

Anycast means that if the attacker attacked the last step in the traceroute then their attack would be spread across CloudFlare's worldwide network, so instead they attacked the second to last step which concentrated the attack on one single point. This wouldn't cause a network-wide outage, but it could potentially cause regional problems.

We carefully select our bandwidth providers to ensure they have the ability to deal with attacks like this. Our direct peers quickly filtered attack traffic at their edge. This pushed the attack upstream to their direct peers, largely Tier 1 networks. Tier 1 networks don't buy bandwidth from anyone, so the majority of the weight of the attack ended up being carried by them. While we don't have direct visibility into the traffic loads they saw, we have been told by one major Tier 1 provider that they saw more than 300Gbps of attack traffic related to this attack. That would make this attack one of the largest ever reported.

The challenge with attacks at this scale is they risk overwhelming the systems that link together the Internet itself. The largest routers that you can buy have, at most, 100Gbps ports. It is possible to bond more than one of these ports together to create capacity that is greater than 100Gbps however, at some point, there are limits to how much these routers can handle. If that limit is exceeded then the network becomes congested and slows down.

Over the last few days, as these attacks have increased, we've seen congestion across several major Tier 1s, primarily in Europe where most of the attacks were concentrated, that would have affected hundreds of millions of people even as they surfed sites unrelated to Spamhaus or CloudFlare. If the Internet felt a bit more sluggish for you over the last few days in Europe, this may be part of the reason why.

In addition to CloudFlare's direct peers, we also connect with other

networks over the so-called Internet Exchanges (IXs). These IXs are, at their most basic level, switches into which multiple networks connect and can then pass bandwidth. In Europe, these IXs are run as non-profit entities and are considered critical infrastructure. They interconnect hundreds of the world's largest networks including CloudFlare, Google, Facebook, and just about every other major Internet company.

Beyond attacking CloudFlare's direct peers, the attackers also attacked the core IX infrastructure on the London Internet Exchange (LINX), the Amsterdam Internet Exchange (AMS-IX), the Frankfurt Internet Exchange (DE-CIX), and the Hong Kong Internet Exchange (HKIX). From our perspective, the attacks had the largest effect on LINX which caused impact over the exchange and LINX's systems that monitor the exchange, as visible through the drop in traffic recorded by their monitoring systems. (Corrected: see below for original phrasing.)

The congestion impacted many of the networks on the IXs, including CloudFlare's. As problems were detected on the IX, we would route traffic around them. However, several London-based CloudFlare users reported intermittent issues over the last several days. This is the root cause of those problems.

The attacks also exposed some vulnerabilities in the architecture of some IXs. We, along with many other network security experts, worked with the team at LINX to better secure themselves. In doing so, we developed a list of best practices for any IX in order to make them less vulnerable to attacks.

Two specific suggestions to limit attacks like this involve making it more difficult to attack the IP addresses that members of the IX use to interchange traffic between each other. We are working with IXs to ensure that: 1) these IP addresses should not be announced as routable across the public Internet; and 2) packets destined to these IP addresses should only be permitted from other IX IP addresses. We've been very impressed with the team at LINX and how quickly they've worked to implement these changes and add additional security to their IX and are hopeful other IXs will quickly follow their lead.

At the bottom of this attack we once again find the problem of open DNS recursors. The attackers were able to generate more than 300Gbps of traffic likely with a network of their own that only had access 1/100th of that amount of traffic themselves. We've written about how these mis-configured DNS recursors as a bomb waiting to go off that literally threatens the stability of the Internet itself. We've now seen an attack that begins to illustrate the full extent of the problem.

While lists of open recursors have been passed around on network security lists for the last few years, on Monday the full extent of the problem was, for the first time, made public. The Open Resolver Project made available the full list of the 21.7 million open resolvers online in an effort to shut them down.

We'd debated doing the same thing ourselves for some time but worried about the collateral damage of what would happen if such a list fell into the hands of the bad guys. The last five days have made clear that the bad guys have the list of open resolvers and they are getting increasingly brazen in the attacks they are willing to launch. We are in full support of the Open Resolver Project and believe it is incumbent on all network providers to work with their customers to close any open resolvers running on their networks.

Unlike traditional botnets which could only generate limited traffic because of the modest Internet connections and home PCs they typically run on, these open resolvers are typically running on big servers with fat pipes. They are like bazookas and the events of the last week have shown the damage they can cause. What's troubling is that, compared with what is possible, this attack may prove to be relatively modest.

As someone in charge of DDoS mitigation at one of the Internet giants emailed me this weekend: "I've often said we don't have to prepare for the largest-possible attack, we just have to prepare for the largest attack the Internet can send without causing massive collateral damage to others. It looks like you've reached that point, so... congratulations!"

At CloudFlare one of our goals is to make DDoS something you only read about in the history books. We're proud of how our network held up under such a massive attack and are working with our peers and partners to ensure that the Internet overall can stand up to the threats it faces.

Correction: The original sentence about the impact on LINX was "From our perspective, the attacks had the largest effect on LINX which for a little over an hour on March 23 saw the infrastructure serving more than half of the usual 1.5Tbps of peak traffic fail." That was not well phrased, and has been edited, with notation in place.

New Book Shares Insights from Steve Jobs' 1st Boss

When Steve Jobs adopted "think different" as Apple's mantra in the late 1990s, the company's ads featured Albert Einstein, Bob Dylan, Amelia Earhart and a constellation of other starry-eyed oddballs who reshaped society.

Nolan Bushnell never appeared in those tributes, even though Apple was riffing on an iconoclastic philosophy he embraced while running video game pioneer Atari in the early 1970s. Atari's refusal to be corralled by the status quo was one of the reasons Jobs went to work there in 1974 as an unkempt, contemptuous 19-year-old. Bushnell says Jobs offended some Atari employees so much that Bushnell eventually told Jobs to work nights when one else was around.

Bushnell, though, says he always saw something special in Jobs, who evidently came to appreciate his eccentric boss, too. The two remained in touch until shortly before Jobs died in October 2011 after a long battle with pancreatic cancer.

That bond inspired Bushnell to write a book about the unorthodox thinking that fosters the kinds of breakthroughs that became Jobs' hallmark as the co-founder and CEO of Apple Inc. Apple built its first personal computers with some of the parts from Atari's early video game machines. After Jobs and Steve Wozniak started Apple in 1976, Apple also adopted parts of an Atari culture that strived to make work seem like play. That included pizza-and-beer parties and company retreats to the beach.

"I have always been pretty proud about that connection," Bushnell said in an interview. "I know Steve was always trying to take ideas and turn them upside down, just like I did."

Bushnell, now 70, could have reaped even more from his relationship with Jobs if he hadn't turned down an offer from his former employee to invest $50,000 in Apple during its formative stages. Had he seized that opportunity, Bushnell would have owned one-third of Apple, which is now worth about $425 billion more than any other company in the world.

Bushnell's newly released book, "Finding The Next Steve Jobs: How to Find, Hire, Keep and Nurture Creative Talent," is the latest chapter in a diverse career that spans more than 20 different startups that he either launched on his own or groomed at Catalyst Technologies, a business incubator that he once ran.

He has often pursued ideas before the technology needed to support them was advanced enough to create a mass market. Bushnell financed Etak, an automobile mapping system created in 1983 by the navigator of his yacht and later sold to Rupert Murdoch's News Corp. Bushnell also dabbled in electronic commerce during the 1980s by launching ByVideo, which took online orders through kiosks set up in airports and other locations. In his most costly mistake, Bushnell lost nearly all of a $28 million investment in Androbot, another 1980s-era startup. It developed 3-foot-tall robots that were supposed to serve the dual role of companion and butler. (Bushnell relied on Apple's computers to control the early models.)

Bushnell's best-known accomplishments came at Atari, which helped launch the modern video game industry with the 1972 release of "Pong," and at the Chuck E Cheese restaurant chain, which specializes in pizza, arcade entertainment and musical performances by animatronic animals. It's an odyssey that led actor Leonardo DiCaprio to obtain the film rights to Bushnell's life for a possible movie starring DiCaprio in the lead role.

While at Atari, Bushnell began to break the corporate mold, creating a template that is now common through much of Silicon Valley. He allowed employees to turn Atari's lobby into a cross between a video game arcade and the Amazon jungle. He started holding keg parties and hiring live bands to play for his employees after work. He encouraged workers to nap during their shifts, reasoning that a short rest would stimulate more creativity when they were awake. He also promised a summer sabbatical every seven years.

He advertised job openings at Atari with taglines such as, "Confusing work with play every day" and "Work harder at having fun than ever before." When job applicants came in for interviews, he would ask brain-teasing questions such as: "What is a mole?"; "Why do tracks run counter-clockwise?" and "What is the order of these numbers: 8, 5, 4, 9, 1, 7, 6, 3, 2?"

Bushnell hadn't been attracting much attention in recent years until Walter Isaacson's best-selling biography on Jobs came out in 2011, just after Jobs' death. It reminded readers of Bushnell's early ties to the man behind the Macintosh computer, iPod, iPhone and iPad.

Suddenly, everyone was asking Bushnell about what it was like to be Jobs' first boss. Publisher Tim Sanders of Net Minds persuaded him to write a book linked to Jobs, even though Bushnell had already finished writing a science fiction novel about a video game hatched through nanotechnology in 2071.

"The idea is to become a best-selling author first and then the rest of my books will be slam dunks," Bushnell said. To get his literary career

rolling, Bushnell relied on veteran ghostwriter Gene Stone, who also has written other books, including "Forks Over Knives," under his own name.

Bushnell’s book doesn’t provide intimate details about what Jobs was like after he dropped out of Reed College in Portland, Ore., and went to work as a technician in 1974 at Atari in Los Gatos, Calif. He had two stints there, sandwiched around a trip to India. During his second stint at Atari, in 1975, Jobs worked on a "Pong" knock-off called "Breakout" with the help of his longtime friend Wozniak, who did most of the engineering work on the video game, even though he wasn’t being paid by Atari. Jobs left Atari for good in 1976 when he co-founded Apple with Wozniak, who had been designing engineering calculators at Hewlett-Packard Co.

Jobs and Bushnell kept in touch. They would periodically meet over tea or during walks to hash out business ideas. After Bushnell moved to Los Angeles with his family 13 years ago, he didn’t talk to Jobs as frequently, though he made a final visit about six months before he died.

There are only a few anecdotes about Bushnell’s interaction with Jobs at Atari and about those meetings around Silicon Valley.

The book instead serves as a primer on how to ensure a company doesn’t turn into a mind-numbing bureaucracy that smothers existing employees and scares off rule-bending innovators such as Jobs.

Bushnell dispenses his advice in vignettes that hammer on a few points. The basics: Make work fun; weed out the naysayers; celebrate failure, and then learn from it; allow employees to take short naps during the day; and don’t shy away from hiring talented people just because they look sloppy or lack college credentials.

Many of these principles have become tenets in Silicon Valley’s laid-back, risk-taking atmosphere, but Bushnell believes they remain alien concepts in most of corporate America.

"The truth is that very few companies would hire Steve, even today," Bushnell writes in his book. "Why? Because he was an outlier. To most potential employers, he’d just seem like a jerk in bad clothing."

Bushnell says he is worried that Apple is starting to lose the magic touch that Jobs brought to the company. It’s a concern shared by many investors, who have been bailing out of Apple’s stock amid tougher competition for the iPhone and the iPad and the lack of a new product line since Tim Cook became the company’s CEO shortly before Jobs’ death. Apple’s market value has dropped by 36 percent, or about $235 billion, from its all-time high reached last September.

The incremental steps that Apple has been taking with the iPod, iPhone and iPad have been fine, Bushnell says, but not enough to prove the company is still thinking differently.

"To really maintain the cutting edge that they live on, they will have to do some radical things that resonate," Bushnell said. "They probably have three more years before they really have to do something big. I hope they are working on it right now."

Bushnell is still keeping busy himself. When he isn’t writing, he is running his latest startup, Brainrush, which is trying to turn the process of learning into a game-like experience. He says he hopes to fix an educational system that he believes is "incorrect, inefficient and

bureaucratic all the things you don’t want to see in your workforce of the future."

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.